(19)日本国特許庁（ＪＰ）

(12) 公開特許公報（A）

(11)特許出願公開番号
特開2000－35929
（P2000－35929A）

(43)公開日 平成12年２月２日(2000.2.2)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
G06F	13/00	351	G06F	13/00	351Z 5B085
	15/00	310		15/00	310D 5B089
H04L	12/24		H04L	11/08	5K030
	12/26			13/00	313 5K035
	29/14				

審査請求 未請求 請求項の数３ ＯＬ （全 ６ 頁）

(21)出願番号 特願平10－202318

(22)出願日 平成10年７月16日(1998.7.16)

(71)出願人 000153465
株式会社日立テレコムテクノロジー
福島県郡山市宇船場向94番地

(72)発明者 藤田 秀樹
福島県郡山市宇船場向94番地 株式会社日立テレコムテクノロジー内

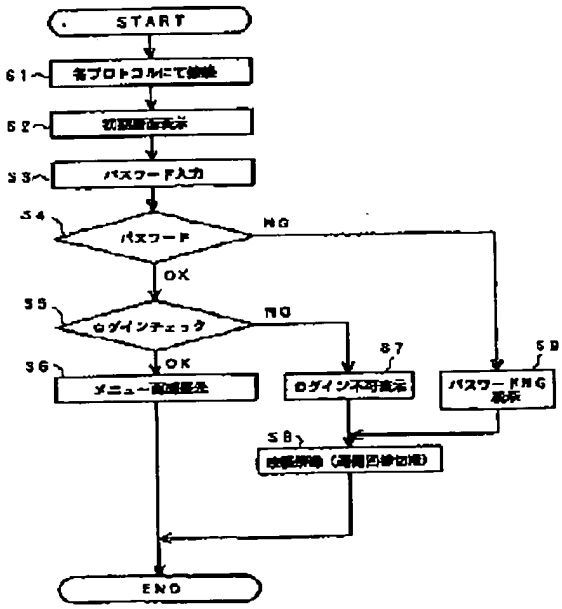
(72)発明者 遠藤 信行
福島県郡山市宇船場向94番地 株式会社日立テレコムテクノロジー内

(74)代理人 100083954
弁理士 青木 輝夫

最終頁に続く

(54)【発明の名称】 通信装置に対する管理端末の接続制御方法

(57)【要約】
【課題】 ネットワーク上に接続された通信装置に対する管理端末の接続制御方法に関し、通信装置へのログイン／ログアウトのセキュリティを向上させることを目的とする。
【解決手段】 ネットワークに接続されている通信装置と通信装置の保守管理を行う管理端末との接続制御方法において、管理端末の画面に初期画面を表示する処理と、初期画面に従って管理端末からパスワードを入力する処理と、入力されたパスワードが正しく他の管理端末がログイン中でないときは管理端末が通信装置にログインして保守作業に入る処理と、入力されたパスワードが正しく他の管理端末がログイン中のときは管理端末にログイン不可情報を表示して接続を解除する処理とからなる。



【特許請求の範囲】
【請求項1】 ネットワークに接続されている通信装置と前記通信装置の保守管理を行う管理端末との接続制御方法において、
前記管理端末の画面に初期画面を表示する処理と、
前記初期画面に従って前記管理端末からパスワードを入力する処理と、
前記入力されたパスワードが正しく他の管理端末がログイン中でないときは前記管理端末が前記通信装置にログインして保守作業に入る処理と、
前記入力されたパスワードが正しく他の管理端末がログイン中のときは前記管理端末にログイン不可情報を表示して接続を解除する処理と、からなることを特徴とする通信装置に対する管理端末の接続制御方法.
【請求項2】 前記ログイン後の保守作業中にネットワークの障害により通信回線が切断されたことを検知すると、前記ログイン状態を自動的に回避して接続を解除することを特徴とする請求項1記載の通信装置に対する管理端末の接続制御方法。
【請求項3】 前記ログイン後の保守作業中に前記管理端末からのキーオペレーションが一定時間以上ないことを検知すると、前記ログイン状態を自動的に回避して接続を解除することを特徴とする請求項1記載の通信装置に対する管理端末の接続制御方法。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、ネットワーク上に接続された通信装置に対する管理端末の接続制御方法に関する。
【0002】
【従来の技術】従来、管理端末から通信装置に対して保守作業をする場合は、特定の管理端末からの保守作業しか可能でなかったため、複数の管理端末からの同時ログインを抑制する機能は必要ではなかった。また、通信回線の障害やオペレーションの誤りによってログアウトを忘れ、ログイン状態のままになってしまう状態を回避する手段もなかった。
【0003】
【発明が解決しようとする課題】現在、通信装置の保守形態の多様化により、通信装置を複数の管理端末から複数の経路を介して保守する必要があるため、複数の管理端末から同時にログインが起きたとき、保守作業の重複を抑制しなければならないという要求がある。
【0004】また、保守作業中の通信回線の障害による通信切断や、オペレーションの誤りによるログアウト忘れにより、通信装置がログイン状態のままになってしまい、どの管理端末からもログインができず、このため保守作業ができないという不都合が生じる。
【0005】本発明は、このような従来の課題を解決するためになされたもので、通信装置へのログイン／ログアウトのセキュリティが向上する通信装置に対する管理端末の接続制御方法を提供することを目的とする。
【0006】
【課題を解決するための手段】本発明の請求項1記載の発明は、ネットワークに接続されている通信装置と通信装置の保守管理を行う管理端末との接続制御方法において、管理端末の画面に初期画面を表示する処理と、初期画面に従って管理端末からパスワードを入力する処理と、入力されたパスワードが正しく他の管理端末がログイン中でないときは管理端末が通信装置にログインして保守作業に入る処理と、入力されたパスワードが正しく他の管理端末がログイン中のときは管理端末にログイン不可情報を表示して接続を解除する処理とからなるものである。
【0007】本発明によれば、ネットワークに接続されている通信装置へ管理端末からログインするときに、通信装置へログインするための初期画面を管理端末に表示し、正しいパスワードを管理端末で入力することによりログインが可能となる。ログインができたときは通信装置の保守を行うメニュー画面を表示して保守作業に入り、ログインができなかったときはパスワードの入力後に他の管理端末がログイン中であることを知らせるメッセージを管理端末に表示し、自動的に通信回線を切断する。
【0008】本発明の請求項2記載の発明は、請求項1記載の発明において、ログイン後の保守作業中にネットワークの障害で通信回線が切断されたことを検知すると、ログイン状態を自動的に回避して接続を解除するものである。
【0009】本発明によれば、ログイン後は通信回線の障害を周期で監視し、ネットワーク障害で通信回線が切断された場合は、ログイン状態を自動的に回避（ログアウト）するように制御する。
【0010】本発明の請求項3記載の発明は、請求項1記載の発明において、ログイン後の保守作業中に管理端末からのキーオペレーションが一定時間以上ないことを検知すると、ログイン状態を自動的に回避して接続を解除するものである。
【0011】本発明によれば、ログイン後は管理端末からのキーオペレーションを監視し、キーオペレーションが一定時間以上ない場合は、ログアウトし忘れと判断してログイン状態を自動的に回避（ログアウト）するように制御する。
【0012】
【発明の実施の形態】図1は、本発明が適用されるネットワークの一例を示す構成図である。同図において、通信装置1はデータや音声を通信するための装置であり、インターフェイス2（イーサネット）を介して管理端末3に接続されている。
【0013】また、通信装置1はインターフェイス4を

介してネットワーク5に接続されている。ネットワーク5としてはATM（非同期転送モード）、ISDN（サービス総合ディジタル通信網）、専用線網等がある。

【0014】ネットワーク5にはリモートルータ6，7およびインターフェイス8，9（イーサネット）を介して管理端末10，11が接続されている。リモートルータ6，7は通信装置1と管理端末10，11とのIPルーティングを可能とするものである。

【0015】また、通信装置1はインターフェイス12（RS-232C）およびモデム13を介して電話網14に接続されている。この電話網14には、モデム15およびインターフェイス16（RS-232C）を介して管理端末17が接続されている。

【0016】管理端末17は通信装置1を管理するための管理端末で、主にパーソナルコンピュータ（PC）をダムターミナルモードにして使用する。他方、管理端末3，10，11は主にUNIXのワークステーションを用いる。

【0017】次に、図2に示すフローチャート図を参照して、ログイン制御の動作について説明する。まず、通信装置1と各管理端末3，10，11，17のいずれかとを各プロトコルによって接続する（ステップS1）。

【0018】これは、図3に示すように、物理インターフェイスによって接続するプロトコルが異なるためで、管理端末3，10，11はTCP/IPのアプリケーションの「rlogin，telnet」を使用して接続を行い、管理端末17は「独自手順」で接続する。

【0019】ステップS1で通信回線またはTCP/IPのセッションが接続されると、接続装置の保守作業をするために初期画面が表示される（ステップS2）。保守者は画面に表示される手順に従い、キー操作をしてパスワードを入力する（ステップS3）。

【0020】次いで、パスワードのチェックを行い（ステップS4）、正解（OK）であれば、他の管理端末がログインしているかをチェックする（ステップS5）。他の管理端末がログインしていなければ、保守作業を行うためのメニュー画面をその管理端末に表示し（ステップS6）、保守作業を可能として処理を終了する。

【0021】他の管理端末が既にログインしている場合は（ステップS5）、ログイン不可のメッセージをその管理端末に表示し（ステップS7）、通信回線またはセッションを切断して通信を終了する（ステップS8）。

【0022】パスワードのチェックの結果（ステップS4）、パスワードが不正解（NG）であれば、パスワードの間違いを示すメッセージをその管理端末に表示し（ステップS9）、通信回線またはセッションを切断して通信を終了する（ステップS8）。

【0023】次に、図4に示すフローチャート図を参照して、保守作業中の障害監視の動作について説明する。なお、監視周期は5秒で行っている。

【0024】まず、通信回線の信号線情報を読み込む（ステップS11）。この処理は図3に示すように、物理インターフェイスがRS-232Cの場合のみである。

【0025】次に、読み込んだ信号線が障害かどうか判定する（ステップS12）。信号線が正常な場合はキー入力があったか判定し（ステップS13）、キー入力がなかった場合はタイムアウト時間になったか判定する（ステップS14）。タイムアウト時間になっていない場合は、タイムカウンタを更新して処理を終了する（ステップS15）。タイムアウト時間は、図3に示すように、接続プロトコルにより異なり、独自手順の場合は30分、TCP/IPの場合は5分である。

【0026】信号線に障害がある場合は（ステップS12）、通信が切断（DR=OFF）されてしまったので、ログアウトの処理を実行し（ステップS16）、通信回線を切断して通信装置1のログイン状態を解除し（ステップS17）、処理を終了する。タイムアウト時間になった場合も（ステップS14）、同様のログアウト処理をする（ステップS16，S17）。

【0027】キー入力があった場合は（ステップS13）、今までカウントアップしてきたタイマカウンタをクリアし（ステップS18）、タイムアウト時間をデフォルトに戻して処理を終了する。

【0028】

【発明の効果】本発明によれば、複数の管理端末からの同時ログインを抑制することにより、複数の管理端末からの保守作業で同時にログインが発生した場合でも、通信装置の保守作業の重複を防ぐことができるという有利な効果が得られる。

【0029】また、ログイン中に発生したネットワーク障害による通信切断やオペレーティングミスによるログアウトの忘れを自動的に感知し、ログイン状態を回避（ログアウト）させることにより、障害に対するセキュリティを向上させることができるという有利な効果が得られる。

【図面の簡単な説明】

【図1】本発明が適用されるネットワークの一例を示す構成図である。

【図2】ログイン制御の動作を説明するフローチャート図である。

【図3】各プロトコルによるログアウト時間を表として示す図である。

【図4】障害監視の動作を説明するフローチャート図である。

【符号の説明】

1　通信装置

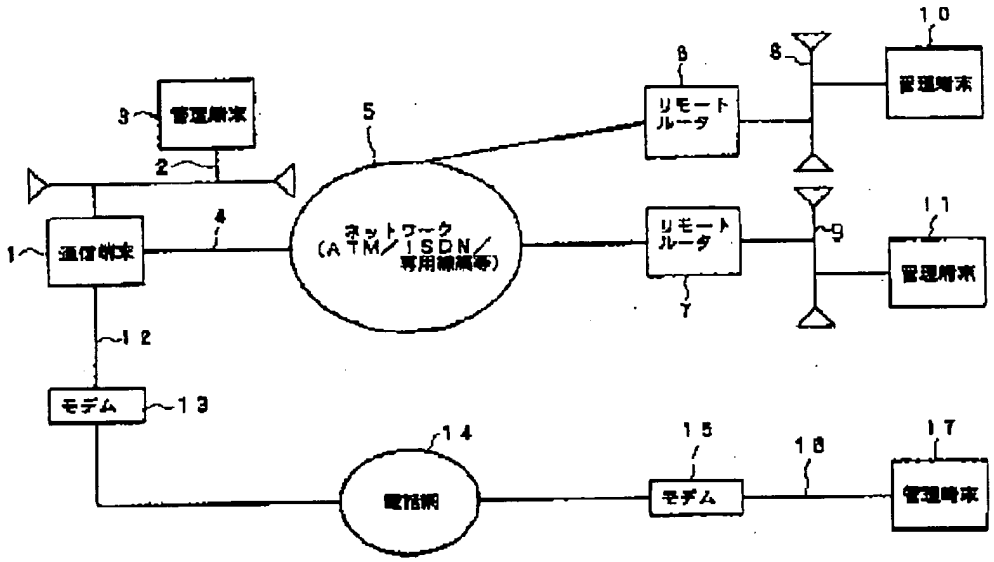
2，8，9　インターフェイス（イーサネット）

3，10，11　管理端末

4　インターフェイス

5 ネットワーク
6, 7 リモートルータ
12, 16 インターフェイス (RS-232C)
17 管理端末
13, 15 モデム
14 電話網

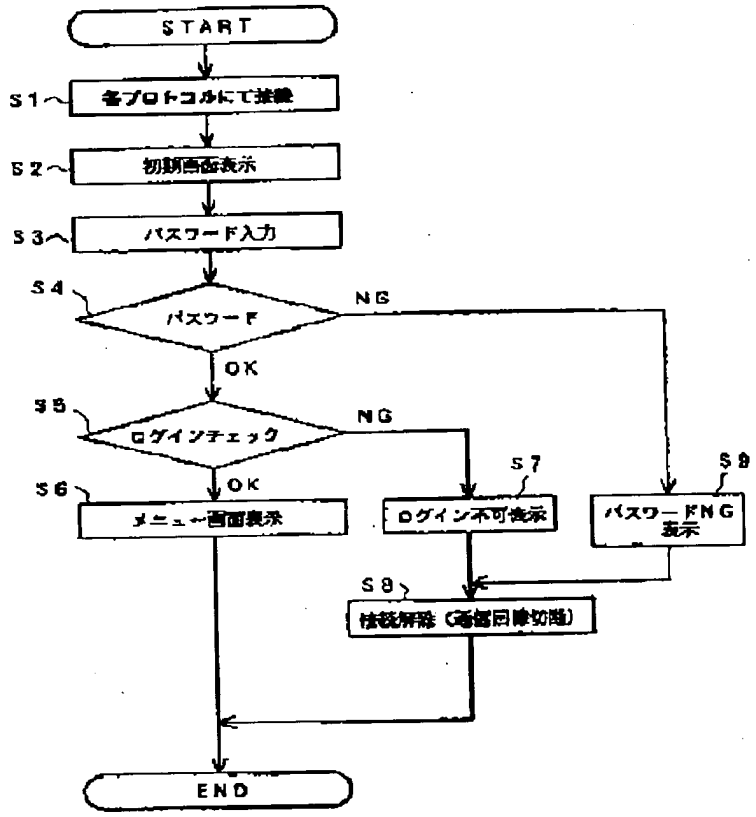
【図1】



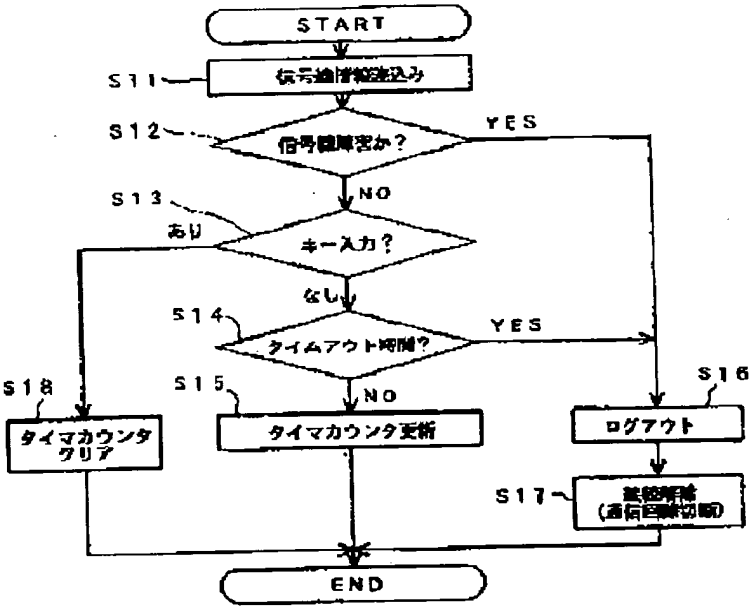
【図3】

物理インターフェース	接続プロトコル	タイムアウト時間	障害監視
RS-232C	独自手順	30分	DR信号線
ATM/ISDN/専用線	TCP/IP (rlogin, telnet)	5分	なし
Ethernet	TCP/IP (rlogin, telnet)	5分	なし

【図2】


START
S1
各プロトコルにて接続
S2
初期画面表示
S3
パスワード入力
S4
パスワード
NG
OK
S5
ログインチェック
NG
OK
S6
メニュー画面表示
S7
ログイン不可表示
S9
パスワードNG表示
S8
情報解除 (各種回線切断)
END

【図4】



フロントページの続き

(72)発明者 鈴木 順子
福島県郡山市字船場向94番地 株式会社日立テレコムテクノロジー内
(72)発明者 大河原 隆行
福島県郡山市字船場向94番地 株式会社日立テレコムテクノロジー内

Fターム(参考) 5B085 AC03 AC16 AE03 BC01
5B089 AA11 AA16 AB02 AB03 AF06 CD09 EB02 EB06 EC06 FF10
5K030 GA17 HC01 HC13 JA10 JT02 LB01 LD20 LE07 MC09
5K035 AA03 AA07 BB03 CC03 DD01 FF04

Customer No 24498
Serial No. 10/511,560

Japanese Kokai Patent Application No. P2000-35929A

Job No.: 228-118191
Ref.: Japanese Patent No. 2000-35929/ PU020131 JP/BJD(Kathleen)/Order No. 8170
Translated from Japanese by the McElroy Translation Company
800-531-9977 customerservice@mcelroytranslation.com

JAPANESE PATENT OFFICE
PATENT JOURNAL
KOKAI PATENT APPLICATION NO. P2000-35929A

Int. Cl.[7]:	G 06 F 13/00 15/00 H 04 L 12/24 12/26 29/14 H 04 L 11/08 13/00
Filing No.:	Hei 10[1998]-202318
Filing Date:	July 16, 1998
Publication Date:	February 2, 2000
No. of Claims:	3 (Total of 6 pages; OL)
Examination Request:	Not filed

CONNECTION CONTROL METHOD FOR MANAGEMENT TERMINAL FOR A COMMUNICATION DEVICE

Inventors:

Hideki Fujita
Hitachi Telecom Technology Ltd.
94 Aza Funabamukai Koriyama-shi,
Fukushima-ken

Nobuyuki Endo
Hitachi Telecom Technology Ltd.
94 Aza Funabamukai Koriyama-shi,
Fukushima-ken

Junko Suzuki
Hitachi Telecom Technology Ltd.
94 Aza Funabamukai Koriyama-shi,
Fukushima-ken

Takayuki Ogawara
Hitachi Telecom Technology Ltd.
94 Aza Funabamukai Koriyama-shi,
Fukushima-ken

Applicant: 000153465
Hitachi Telecom Technology Ltd.
94 Aza Funabamukai Koriyama-shi,
Fukushima-ken

Agent: 100083954
Tetsuo Aoki, patent attorney

[There are no amendments to this patent.]

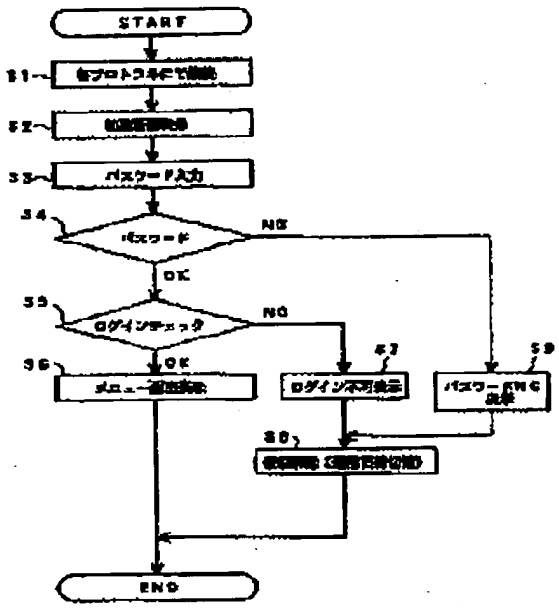
Abstract

Problem

With respect to a connection control method for a management terminal for a communication device connected to a network, the objective is to improve the security of login to/logout from the communication device.

Means to solve

For a connection control method for a communication device connected to a network and a management terminal that performs maintenance for the communication device, a method comprised of a process wherein an initial screen is displayed on the screen of the management terminal; a process wherein a password is input from the management terminal according to the initial screen; a process wherein, when the login password is correct and another management terminal is not logged in, the management terminal is logged in to the communication device and the maintenance work ensues; and a process wherein, when the login password is correct and another management terminal is logged in, information indicating that login is not possible is displayed at the management terminal and the connection is released.



Key: S1 Connect according to respective protocols
S2 Display initial screen
S3 Input password
S4 Password
S5 Check login
S6 Display menu screen
S7 Display indicating login not possible
S8 Release connection (disconnect communication line)
S9 Display indicating password is NG

Claims

1. For a connection control method for a communication device connected to a network and a management terminal that performs maintenance for the aforementioned communication device,

a connection control method for a management terminal for a communication device characterized in that it is comprised of a process wherein an initial screen is displayed on the screen of the aforementioned management terminal;

a process wherein a password is input from the aforementioned management terminal according to the aforementioned initial screen;

a process wherein, when the aforementioned login password is correct and another management terminal is not logged in, the aforementioned management terminal is logged in to the aforementioned communication device and the maintenance work ensues;

and a process wherein, when the aforementioned login password is correct and another management terminal is logged in, information indicating that login is not possible is displayed at the aforementioned management terminal and the connection is released.

2. The connection control method for a management terminal for a communication device recorded in Claim 1, characterized in that when it is detected that the communication line is disconnected due to a network disturbance during the aforementioned maintenance work after the login, the aforementioned login state is automatically prohibited and the connection is released.

3. The connection control method for a management terminal for a communication device recorded in Claim 1, characterized in that during the aforementioned maintenance work after the login, when it is detected that no keys have been operated from the aforementioned management terminal for a fixed period of time, the aforementioned login state is automatically prohibited and the connection is released.

Detailed explanation of the invention

[0001]

Industrial application field

The present invention pertains to a connection control method for a management terminal for a communication device connected to a network.

[0002]

Prior art

Conventionally when maintenance work for a communication device has been performed from a management terminal, it has been possible to perform the maintenance work only from a specific maintenance terminal; therefore, a function to control simultaneous login from multiple management terminals has not been required. Moreover, there has not been a means of preventing a situation wherein an operator forgets to log out due to operational error or a disturbance in the communication lines, thus preserving the logged in status.

[0003]

Problems to be solved by the invention

Currently, due to the proliferation in the forms of maintenance for a communication device, it has become necessary to perform maintenance for a communication device from

multiple management terminals through multiple routes; therefore, it is necessary to prevent redundant maintenance work when logins from multiple maintenance terminals occur simultaneously.

[0004]

Moreover, there is a problem in that during maintenance work if an operator forgets to log out due to operational error or interrupted communication resulting from a disturbance in a communication line, the logged in status is preserved, making it impossible to log in from any management terminal and making it impossible to perform maintenance work.

[0005]

The present invention was devised to solve such problems, and its objective is to offer a connection control method for a management terminal for a communication device wherein the security with respect to login to/logout from the communication device is improved.

[0006]

Means to solve the problems

For a connection control method for a communication device connected to a network and a management terminal that performs maintenance for the communication device, the invention recorded in Claim 1 of the present invention is comprised of a process wherein an initial screen is displayed on the screen of the management terminal; a process wherein a password is input from the management terminal according to the initial screen; a process wherein, when the login password is correct and another management terminal is not logged in, the management terminal is logged in to the communication device and the maintenance work ensues; and a process wherein, when the login password is correct and another management terminal is logged in, information indicating that login is not possible is displayed at the management terminal and the connection is released.

[0007]

By means of the present invention, when a login from a management terminal to a communication device connected to a network occurs, an initial screen for the purpose of logging into the communication device is displayed on the screen of the aforementioned management terminal, and the login is enabled by input of the correct password to the management terminal. When login is achieved, a menu screen, with which maintenance work for the communication device is performed, is displayed and maintenance work ensues; when login is not possible, after the password is input, a message is displayed on the management terminal

indicating that another management terminal is logged in, and the communication line is automatically disconnected.

[0008]

For the invention recorded in Claim 1, the invention recorded in Claim 2 of the present invention is one wherein, when it is detected that the communication line is disconnected due to a network disturbance during the maintenance work after the login, the login state is automatically prohibited and the connection is released.

[0009]

By means of the present invention, the control is such that subsequent to the login, monitoring of the communication line for disturbances is performed periodically, and if the communication line is disconnected due to a network disturbance, the login state is automatically prohibited (log out is implemented).

[0010]

For the invention recorded in Claim 1, the invention recorded in Claim 3 of the present invention is one wherein, during the maintenance work after the login, when it is detected that no keys have been operated from the management terminal for a fixed period of time, the login state is automatically prohibited and the connection is released.

[0011]

By means of the present invention, the control is such that subsequent to login, monitoring of the operation of the keys at the management terminal is performed, and if they are not operated for a fixed period of time, it is assumed that the operator has forgotten to log out and the login state is automatically prohibited (log out is implemented).

[0012]

Embodiment of the invention

Figure 1 illustrates the structure of one example of a network to which the present invention applies. In the figure, communication device 1 is a device for communicating data or audio, and it is connected to a management terminal 3 through an interface 2 (ethernet).

[0013]

Moreover, communication device 1 is connected to a network 5 through an interface 4. Network 5 can be ATM (asynchronous transmission mode), an ISDN (integrated service digital communication network), a dedicated line network, or the like.

[0014]

Management terminals 10, 11 are connected to network 5 through remote routers 6, 7 and interfaces 8, 9 (ethernet). Remote routers 6, 7 enable IP routing of communication device 1 and management terminals 10, 11.

[0015]

Moreover, communication device 1 is connected to a telephone network 14 through an interface 12 (RS-232C) and a modem 13. A management terminal 17 is connected to this telephone network 14 through a modem 15 and an interface 16 (RS-232C).

[0016]

Management terminal 17 is a management terminal for the purpose of managing communication device 1; generally a personal computer (PC) is placed in dumb terminal mode and used for this purpose. On the other hand, UNIX work stations are generally used for management terminals 3, 10, 11.

[0017]

Next, the login control operation will be explained with reference to the flow chart shown in Figure 2. First, one of various management terminals 3, 10, 11, 17 is connected to communication device 1 by means of the respective protocol (Step S1).

[0018]

As shown in Figure 3, because the connection protocol differs according to the physical interface, management terminals 3, 10, 11 connect using a TCP/IP application "rlogin, telnet," and management terminal 17 connects with a "unique procedure."

[0019]

When a communication line or a TCP/IP session is connected at Step S1, the initial screen for the purpose of performing maintenance work for the communication device is displayed (Step S2). The maintenance worker follows the procedure displayed on the screen and operates the keys to input a password (Step S3).

[0020]

Next, the password is checked (Step S4), and if it is correct (OK), a check is made as to whether another management terminal is logged in (Step S5). If another management terminal is not logged in, a menu screen for the purpose of performing maintenance work is displayed on the management terminal (Step S6), and the process ends with maintenance work capable of being performed.

[0021]

If another management terminal is already logged in (Step S5), a message indicating that login is not possible is displayed on the management terminal (Step S7), the communication line or session is disconnected, and communication ends (Step S8).

[0022]

Based on the password check, if the password is incorrect (NG), a message indicating password error is displayed on that management terminal (Step S9), and the communication line or session is disconnected, and communication ends (Step S8).

[0023]

Next, the operation to monitor for disturbances during maintenance work will be explained with reference to the flow chart in Figure 4. The monitoring interval is 5 seconds.

[0024]

First, signal information for the communication line is read (Step S11). As shown in Figure 3, this process occurs only when the physical interface is an RS-232C.

[0025]

Next it is determined whether there is a disturbance with respect to the signal line that was read (Step S12). If the signal line is normal, it is determined whether a key input operation has occurred (Step S13). If there is no key input, it is determined whether the timeout time has arrived (Step S14). If the timeout time has not arrived, the time counter is updated and the process ends (Step S15). As shown in Figure 3, the timeout time differs according to the connection protocol; for the unique procedure it is 30 minutes, and for TCP/IP it is 5 minutes.

[0026]

When there is a disturbance in the signal line (Step S12), communication is disconnected (DR = OFF), so the logout process is executed (Step S16), the communication line is disconnected, the login state of communication device 1 is released (Step S17), and the process ends. When the timeout time arrives (Step S14), the same logout process is executed (Step S16, S17).

[0027]

When a key input has occurred (Step S13), the current count on the time counter is cleared (Steps S18), the timeout time is returned to its default value, and the process ends.

[0028]

Effect of the invention

By means of the present invention, an advantageous result is obtained in that simultaneous login from multiple management terminals is prevented; thus even if simultaneous login from multiple management terminals occurs [sic] with the maintenance work, it is possible to prevent duplication of communication device maintenance work.

[0029]

Moreover, an advantageous result is obtained in that if communication is interrupted due to a network disturbance during login or if an operator mistakenly forgets to log out, this is automatically detected, and by prohibiting the login state (logging out) it is possible to improve security with respect to such disturbances.

Brief description of the figures

Figure 1 illustrates the structure of one example of a network to which the present invention applies.

Figure 2 is a flow chart for the purpose of explaining the login control operation.

Figure 3 is a table of the logout time according to each protocol.

Figure 4 is a flow chart for the purpose of explaining the obstruction monitoring method.

Explanation of symbols

1	Communication device
2, 8, 9	Interface (ethernet)
3, 10, 11	Management terminal
4	Interface

5	Network
6, 7	Remote router
12, 16	Interface (RS-232C)
17	Management terminal
13, 15	Modem
14	Telephone network

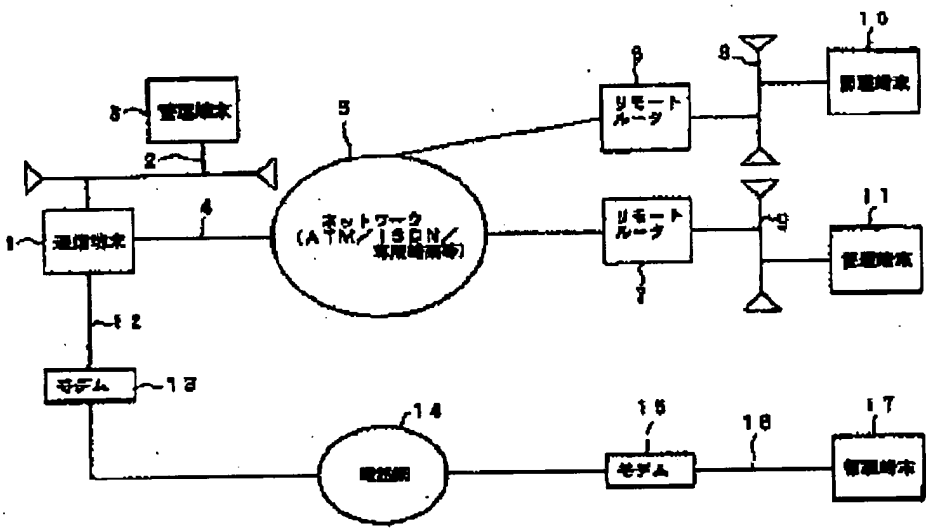


Figure 1

Key:		
	1	Communication device
	3, 10, 11, 17	Management terminal
	5	Network (ATM, ISDN, dedicated line network, etc.)
	6, 7	Remote router
	13, 15	Modem
	14	Telephone network

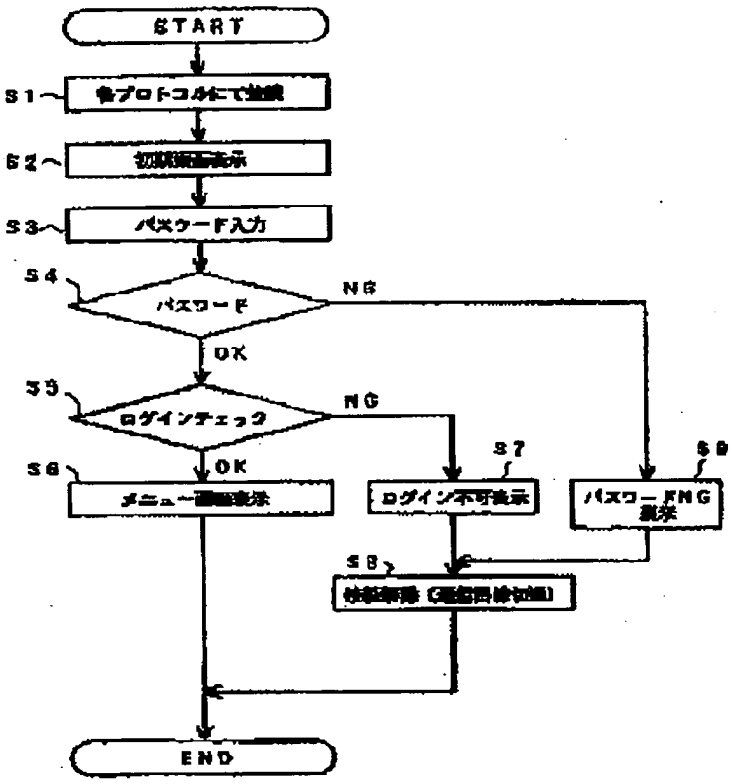


Figure 2

Key:
- S1 Connect according to respective protocols
- S2 Display initial screen
- S3 Input password
- S4 Password
- S5 Check login
- S6 Display menu screen
- S7 Display indicating login not possible
- S8 Release connection (disconnect communication line)
- S9 Display indicating password is NG